UNITED
NATIONS

A

General Assembly

Distr.
LIMITED

A/CN.9/WG.IV/WP.76
25 May 1998

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-third session
New York, 29 June - 10 July 1998

DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Note by the Secretariat

CONTENTS

	Paragraphs	Page
INTRODUCTION	1-8	3
I. GENERAL REMARKS	9-11	5
II. DRAFT PROVISIONS ON DIGITAL SIGNATURES, OTHER ELECTRONIC SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES	12-50	5
CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS	12-15	5
CHAPTER II. ELECTRONIC SIGNATURES	16-38	6
Section I. Electronic signatures in general	16-22	6
Article 1. Definitions	16-20	6
Article 2. Effect of electronic signature	21	10

V.98-53824

	Paragraphs	Page
Section II. [Enhanced][Secure] electronic signatures . .	22-30	11
Article 3. Presumption of signing	22-23	11
Article 4. Presumption of attribution	24	11
Article 5. Presumption of integrity	25-26	12
Article 6. Pre-determination of [enhanced] [secure] electronic signature	27	13
Article 7. Liability for [enhanced][secure] electronic signature	28-30	13
Section III. Digital signatures supported by certificates	31-38	14
Article 8. Contents of [enhanced][secure] certificate	31	14
Article 9. Effect of digital signatures supported by certificates	32-38	15
CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES	39-47	18
Article 10. Undertaking upon issuance of certificate	39	18
Article 11. Contractual liability	40	19
Article 12. Liability of the certification authority to parties relying on certificate	41	20
General remark regarding draft articles 13 to 16	42	21
Article 13. Revocation of certificate	43	21
Article 14. Suspension of certificate	44	23
Article 15. Register of certificates	45-46	23
Article 16. Relations between parties relying on certificates and certification authorities	47	24
CHAPTER IV. FOREIGN ELECTRONIC SIGNATURES . .	48-50	26
Article 17. Provision of services by foreign certification authorities	48	26
Article 18. Endorsement of foreign certificates by domestic certification authorities	49	27
Article 19. Recognition of foreign certificates	50	27

INTRODUCTION

1. The Commission, at its twenty-ninth session (1996), decided to place the issues of digital signatures and certification authorities on its agenda. The Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics. It was agreed that work to be carried out by the Working Group at its thirty-first session could involve the preparation of draft rules on certain aspects of the above-mentioned topics. The Working Group was requested to provide the Commission with sufficient elements for an informed decision to be made as to the scope of the uniform rules to be prepared. As to a more precise mandate for the Working Group, it was agreed that the uniform rules to be prepared should deal with such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers and third parties in the context of the use of certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. [1]

2. At its thirtieth session (1997), the Commission had before it the report of the Working Group on the work of its thirty-first session (A/CN.9/437). As to the desirability and feasibility of preparing uniform rules on issues of digital signatures and certification authorities, the Working Group indicated to the Commission that it had reached consensus as to the importance of, and the need for, working towards harmonization of law in that area. While it had not made a firm decision as to the form and content of such work, it had come to the preliminary conclusion that it was feasible to undertake the preparation of draft uniform rules at least on issues of digital signatures and certification authorities, and possibly on related matters. The Working Group recalled that, alongside digital signatures and certification authorities, future work in the area of electronic commerce might also need to address: issues of technical alternatives to public-key cryptography; general issues of functions performed by third-party service providers; and electronic contracting (A/CN.9/437, paras. 156-157). With respect to the issue of incorporation by reference, the Working Group concluded that no further study by the Secretariat was needed, since the fundamental issues were well known and it was clear that many aspects of battle-of-forms and adhesion contracts would need to be left to applicable national laws for reasons involving, for example, consumer protection and other public-policy considerations. The Working Group was of the opinion that the issue should be dealt with as the first substantive item on its agenda, at the beginning of its next session (A/CN.9/437, para. 155).

3. The Commission expressed its appreciation for the work already accomplished by the Working Group at its thirty-first session, endorsed the conclusions reached by the Working Group, and entrusted the Working Group with the preparation of uniform rules on the legal issues of digital signatures and certification authorities (hereinafter referred to as "the Uniform Rules").

4. With respect to the exact scope and form of the Uniform Rules, the Commission generally agreed that no decision could be made at this early stage of the process. It was felt that, while the Working Group might appropriately focus its attention on the issues of digital signatures in view of the apparently predominant role played by public-key cryptography in the emerging electronic-commerce practice, the Uniform Rules should be consistent with the media-neutral

approach taken in the UNCITRAL Model Law on Electronic Commerce. Thus, the Uniform Rules should not discourage the use of other authentication techniques. Moreover, in dealing with public-key cryptography, the Uniform Rules might need to accommodate various levels of security and to recognize the various legal effects and levels of liability corresponding to the various types of services being provided in the context of digital signatures. With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the establishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought. [2]

5. The Working Group began the preparation of the Uniform Rules at its thirty-second session on the basis of a note prepared by the Secretariat (A/CN.9/WG.IV/WP.73). The Secretariat was requested to prepare, on the basis of the deliberations and conclusions of the Working Group, a set of revised provisions, with possible variants, for consideration by the Working Group at a future session (for the report on the work of that session, see A/CN.9/446). With respect to incorporation by reference, the Working Group adopted the text of a draft provision, decided that it should be presented to the Commission for review and possible insertion as a new article 5bis of the UNCITRAL Model Law on Electronic Commerce and requested the Secretariat to prepare an explanatory note to be added to the Guide to Enactment of the Model Law (A/CN.9/446, para. 24).

6. This note contains the revised draft provisions prepared pursuant to the deliberations and decisions of the Working Group and also pursuant to the deliberations and decisions of the Commission at its thirtieth session, as reproduced above. In particular, the draft provisions are based on the working assumption adopted by the Working Group that its work in the area of digital signatures would take the form of draft statutory provisions (A/CN.9/437, para. 27). They are also intended to reflect the decision made by the Working Group at its thirty-first session that possible uniform rules in the area of digital signatures should be derived from article 7 of the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law") and should be considered as setting out a manner in which a reliable method could be used "to identify a person" and "to indicate that person's approval" of the information contained in a data message.

7. In the preparation of this note, the Secretariat was assisted by a group of experts, comprising both experts invited by the Secretariat and experts designated by interested governments and international organizations.

8. In line with the applicable instructions relating to the stricter control and limitation of United Nations documents, the explanatory remarks to the draft provisions have been kept as brief as possible. Additional explanations will be provided orally at the session.

I. GENERAL REMARKS

9. The purpose of the Uniform Rules, as reflected in the draft provisions set forth in part II of this note, is to facilitate the increased use of electronic signatures in international business transactions. Drawing on the many legislative instruments already in force or currently being prepared in a number of countries, these draft provisions aim at preventing disharmony in the legal rules applicable to electronic commerce by providing a set of standards on the basis of which the legal effect of digital signatures and other electronic signatures may become recognized, with the possible assistance of certification authorities, for which a number of basic rules are also provided.

10. Focused on the private-law aspects of commercial transactions, the Uniform Rules do not attempt to solve all the questions that may arise in the context of the increased use of electronic signatures. In particular, the Uniform Rules do not deal with aspects of public policy, administrative law, consumer law or criminal law that may need to be taken into account by national legislators when establishing a comprehensive legal framework for electronic signatures.

11. Based on the Model Law, the Uniform Rules are intended to reflect in particular: the principle of media-neutrality; an approach under which functional equivalents of traditional paper-based concepts and practices should not be discriminated against; and extensive reliance on party autonomy. They are intended for use both as minimum standards in an "open" environment (i.e., where parties communicate electronically without prior agreement) and as default rules in a "closed" environment (i.e., where parties are bound by pre-existing contractual rules and procedures to be followed in communicating by electronic means).

II. DRAFT PROVISIONS ON DIGITAL SIGNATURES, OTHER ELECTRONIC SIGNATURES, CERTIFICATION AUTHORITIES AND RELATED LEGAL ISSUES

CHAPTER I. SPHERE OF APPLICATION AND GENERAL PROVISIONS

12. In considering the draft provisions proposed for inclusion in the Uniform Rules, the Working Group may wish to consider more generally the relationship between the Uniform Rules and the Model Law. In particular, the Working Group might wish to make proposals to the Commission as to whether uniform rules on digital signatures should constitute a separate legal instrument or whether they should be incorporated in an extended version of the Model Law, for example as a new part III of the Model Law.

13. If the Uniform Rules are prepared as a separate instrument, it is submitted that they will need to incorporate provisions along the lines of articles 1 (Sphere of application), 2(a),(c) and (e) (Definitions of "data message", "originator" and "addressee"), 3 (Interpretation), 7 (Signature) and 13 (Attribution of data messages) of the Model Law. While those articles are not reproduced in this note, it should be noted that the draft provisions of the Uniform Rules have been prepared by the Secretariat based on the assumption that such provisions would form

part of the Uniform Rules. With respect to the sphere of application of the Uniform Rules, it should be borne in mind that under article 1 of the Model Law, transactions involving consumers, while not the focus of the Uniform Rules, would not be excluded from their sphere of application unless the law applicable to consumer transactions in the enacting State conflicted with the Uniform Rules.

14. As to the question of party autonomy, a mere reference to article 4 (Variation by agreement) of the Model Law may not suffice to provide a satisfactory solution, in view of the fact that article 4 establishes a distinction between those provisions of the Model Law that may be freely varied by contract and those provisions that should be regarded as mandatory unless variation by agreement is authorized by the law applicable outside the Model Law. With respect to electronic signatures, the practical importance of "closed" networks makes it necessary to provide wide recognition of party autonomy. However, public policy restrictions on freedom of contract, including laws protecting consumers from overreaching contracts of adhesion, may also need to be taken into consideration. The Working Group may thus wish to include in the Uniform Rules a provision along the lines of article 4(1) of the Model Law to the effect that, except as otherwise provided by the Uniform Rules or other applicable law, electronic signatures and certificates issued, received or relied upon in accordance with procedures agreed among the parties to a transaction are given the effect specified in the agreement. In addition, the Working Group might consider establishing a rule of interpretation to the effect that, in determining whether a certificate, an electronic signature or a data message verified with reference to a certificate, is sufficiently reliable for a particular purpose, all relevant agreements involving the parties, any course of conduct among them, and any relevant trade usage should be taken into account.

15. In addition to the above-mentioned provisions, the Working Group may wish to consider whether a preamble should clarify the purpose of the Uniform Rules, namely to promote the efficient utilization of digital communication by establishing a security framework and by giving written and digital messages equal status as regards their legal effect.

CHAPTER II. ELECTRONIC SIGNATURES

Section I. Electronic signatures in general

Article 1. Definitions

For the purposes of these Rules:

(a) "Electronic signature" means data in electronic form in, affixed to, or logically associated with, a data message, and [that may be] used to [identify the signer of the data message and indicate the signer's approval of the information contained in the data message][satisfy the conditions set forth in article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce];

(b) "[Enhanced][Secure] electronic signature" means an electronic signature which [is created and][as of the time it was made] can be verified through the application of a security procedure or combination of security procedures that ensures that such electronic signature:

(i) is unique to the signer [for the purpose for][within the context in] which it is used;

(ii) can be used to identify objectively the signer of the data message;

(iii) was created and affixed to the data message by the signer or using a means under the sole control of the signer; [and]

[(iv) was created and is linked to the data message to which it relates in a manner such that any change in the data message would be revealed].

(c) Variant A

"Digital signature" means an electronic signature created by transforming a data message using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key, such that any person having the initial untransformed data message, the encrypted transformation, and the signer's corresponding public key can [accurately] determine:

(i) whether the transformation was created using the private key that corresponds to the signer's public key; and

(ii) whether the initial data message has been altered since the transformation was made.

Variant B

"Digital signature" is a cryptographic transformation (using an asymmetric cryptographic technique) of the numerical representation of a data message, such that any person having the data message and the relevant public key can determine:

(i) that the transformation was created using the private key corresponding to the relevant public key; and

(ii) that the data message has not been altered since the cryptographic transformation.

(d) "Certification authority" means any person who, or entity which, in the course of its business, engages in issuing [identity] certificates in relation to cryptographic keys used for the purposes of digital signatures. [This definition is subject to any applicable law which requires a certification authority to be licensed, to be accredited, or to operate in a manner specified in such law.]

(e) "[Identity] certificate" means a data message or other record which is issued by a certification authority and which purports to confirm the identity [or other significant characteristic] of a person or entity who holds a particular key pair.

(f) "[Enhanced][Secure] certificate" means a[n identity] certificate issued for the purpose of supporting [enhanced][secure] electronic signatures.

(g) "Certification practice statement" means a statement published by a certification authority that specifies the practices that the certification authority employs in issuing and otherwise handling certificates.

(h) "Signer" means the person by whom, or on whose behalf, [an electronic signature is used][data is used as an electronic signature].

References

A/CN.9/446, paras. 27-46 (draft article 1), 62-70 (draft article 4), 113-131 (draft article 8), 132-133 (draft article 9);
A/CN.9/WG.IV/WP.73, paras. 16-27, 37-38, 50-57, and 58-60;
A/CN.9/437, paras. 29-50 and 90-113 (draft articles A, B and C); and
A/CN.9/WG.IV/WP.71, paras. 52-60.

Remarks

Definitions of "electronic signature" and "[enhanced][secure] electronic signature"

16. Pursuant to the decision made by the Working Group at its thirty-second session (A/CN.9/446, para. 30), the definition of "electronic signature" refers to article 7 of the Model Law. Depending on the decision to be made with respect to the relationship between the Uniform Rules and the Model Law, the provisions of article 7(1)(a) of the Model Law may need to be stated in full.

17. The distinction between a broad notion of "electronic signature" and a narrower category (provisionally called "enhanced" or "secure" electronic signature) has been maintained with a view to emphasizing the differences in the legal status of two types of procedures. On the one hand, a wide range of unspecified authentication techniques (labelled as "electronic signatures") could obtain legal recognition as a legally significant signature, provided that they met the reliability test set forth in article 7(1)(b) of the Model Law, which would need to be established after the electronic signature had been used, and would typically require the intervention of a judge, arbitrator, or other trier of fact. On the other hand, a number of authentication techniques designated through administrative procedures to be defined by each enacting State or as a result of express agreement between the parties would enjoy advance recognition as functional equivalents to hand-written signatures.

Definition of "digital signature"

18. The category of "digital signatures" is not defined as a subset of "enhanced" electronic signatures. This is intended to reflect the fact that, although in most situations "digital" techniques (with or without reliance on certification authorities) would be used to produce the legal effects envisaged for the more "secure" category of electronic signatures, such techniques could also be used in a less specific context. The definition of "digital signature" is thus intended to emphasize the media-neutral character of the Uniform Rules.

Definition of "certification authority"

19. The Uniform Rules do not contain any requirement as to the standards to be met by certification authorities before they are allowed to operate. The issue was discussed by the Working Group at previous sessions and is also dealt with in draft article 19. Should it be regarded necessary to provide guidance to enacting States, either in the text of the Uniform Rules or in a guide to enactment, attention might be given to the following example of a possible provision:

Certification authorities must:

(a) possess the reliability necessary for offering certification services;

(b) employ personnel which possess the expert knowledge, experience, and qualifications necessary for the offered services;

(c) use trustworthy systems and generally acknowledged hardware and software adequate for the type of service and degree of security offered;

(d) have sufficient financial resources to operate in conformity with [these Rules];

(e) record all relevant information concerning a[n] [enhanced][secure] certificate for an appropriate period of time, in particular to be able to provide evidence of certification in the context of a lawsuit. Such recording may be done electronically;

(f) publish all relevant information concerning the proper and secure use of certification services and establish procedures for complaints and dispute settlement; and

(g) publish with regard to the services available to the public, all relevant information concerning used procedures and applied practices, the terms and conditions of the contracts, in particular the liability obligations they undertake, as well as the complaints and dispute settlement procedures they apply; publication shall be accessible in an appropriate and easy manner.

Definitions of "[identity] certificate and "[enhanced][secure] certificate"

20. The definitions in subparagraphs (e) and (f) draw on the suggestion made at the thirty-second session of the Working Group to distinguish the cases where digital signatures were used

for the purposes of international trade transactions with the intent to sign (i.e., to identify the signer and link the signer with the information being signed) from other uses of digital signatures, e.g., to establish the level of authority of a person ("authority certificates") (see A/CN.9/446, para. 72). While the provisions contained in Chapter III of the Uniform Rules deal mostly with digital signature techniques as a means of establishing pre-determined equivalency with hand-written signatures, the Working Group may wish to discuss the extent to which digital signature techniques should be dealt with in other contexts. Should the Uniform Rules focus on digital signatures as equivalent to hand-written signatures, there might be no need to distinguish between "certificates", "identity certificates" and "[enhanced] [secure] certificates". It may be recalled that any lower-security use of digital signatures could also be covered by the general provisions of draft article 2.

Article 2. Effect of electronic signature

(1) With respect to a data message authenticated by means of an electronic signature [other than a secure electronic signature], the electronic signature satisfies any legal requirement for a signature if the electronic signature is as reliable as appropriate for the purpose for which the electronic signature was used, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the legal requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) Unless expressly provided elsewhere in [this Law], electronic signatures that are not [enhanced][secure] electronic signatures are not subject to the regulations, standards, or licensing procedures established by ... [*the State-specified organs or authorities referenced in article*] or to the presumptions created by articles 4, 5 and 6.

(4) The provisions of this article do not apply to the following: [...].

References

A/CN.9/446, paras. 27-46 (draft article 1).

Remarks

21. Draft article 2 is intended to deal with the legal effect of electronic signatures that do not meet the requirements set forth for the recognition of the "enhanced" or "secure" status. Consistent with the mandate received from the Commission and with views expressed at the thirty-second session of the Working Group (see A/CN.9/446, paras. 4 and 45), the purpose of the draft article is to ensure the media-neutrality of the Uniform Rules, to make it clear that the use of low-security authentication techniques is not prohibited, and to provide appropriate recognition of party autonomy, without allowing parties to derogate from mandatory rules of law relating to signatures. Paragraphs (1), (2) and (4) merely restate provisions contained in

article 7 of the Model Law. Paragraph (3) addresses the distinction to be drawn between the legal effects of electronic signatures in general, as opposed to "enhanced" or "secure" authentication techniques.

Section II. [Enhanced][Secure] electronic signatures

Article 3. Presumption of signing

(1) A data message is presumed to have been signed [if][as of the time] a[n] [enhanced] [secure] electronic signature is affixed to the data message.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/446, paras. 47-48 (draft article 2) and 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 28-36; and
A/CN.9/437, paras. 43, 48 and 92.

Remarks

22. The draft article creating a presumption that a data message is to be regarded as "signed" if it is authenticated by a secure electronic signature has been redrafted pursuant to a view expressed at the thirty-second session, that the relationship between the definition of a secure electronic signature and the presumptions flowing from the use of such secure electronic signature needed to be clarified (see A/CN.9/446, para. 34).

23. The Uniform Rules contain no definition of "signature" and no indication of any specific legal effects attached to any such "signature". Under draft article 3, the legal effect of a signature is to be determined by reference to domestic law outside the Uniform Rules.

Article 4. Presumption of attribution

(1) A[n] [enhanced][secure] electronic signature is presumed to be that of the person by whom, or on whose behalf, it purports to have been used,

Variant A — unless the purported signer establishes that the [enhanced][secure] electronic signature was affixed without authorization.

Variant B — provided that the relying party establishes that the security procedure or combination of security procedures used to verify the signature was

(a) commercially reasonable under the circumstances;

(b) applied by the relying party in a trustworthy manner, and

(c) relied upon by the relying party reasonably and in good faith.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/446, paras. 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 33-36;
A/CN.9/437, paras. 118-124 (draft article E); and
A/CN.9/WG.IV/WP.71, paras. 64-65.

Remarks

24. Variant A deals with attribution of an electronic signature by allocating the burden of proof along the lines suggested at the thirty-second session of the Working Group (see A/CN.9/446, para. 60). Variant B places the burden of proof on the relying party.

Article 5. Presumption of integrity

(1) If the purported signer has used a security procedure which is capable of providing [reliable] evidence that a data message or any [[enhanced][secure] electronic] [electronic] signature thereon has not been changed since the time the security procedure was applied to the data message or to any signature, then it is presumed [in the absence of evidence to the contrary,] that the data message or the signature has not been changed.

(2) The provisions of this article do not apply to the following: [...].

References

A/CN.9/446, paras. 47-48 (draft article 2);
A/CN.9/WG.IV/WP.73, paras. 28-32; and
A/CN.9/437, paras. 43, 48 and 92.

Remarks

25. The previous draft of the Uniform Rules referred to verification of the integrity of the data message as an element of the definition of a "secure electronic signature". It has been brought to the attention of the Secretariat that verification of the integrity of the data message might be performed through separate procedures. Moreover, it is conceivable that certain authentication techniques would achieve the high level of security required under the definition of "enhanced" electronic signatures without verifying the integrity of the data message.

26. Should the Working Group find it more appropriate, the provisions of draft articles 3, 4 and 5 might be reworded to establish legal effects instead of presumptions.

Article 6. Pre-determination of [enhanced][secure] electronic signature

(1) A security procedure or a combination of security procedures satisfies the requirements of an [enhanced][secure] electronic signature if it is so declared by ...*[the organ or authority specified by the enacting State as competent to make such declaration...]*.

(2) As between the person signing a data message and any person relying on the signed message, a security procedure or a combination of security procedures is deemed to fulfil the requirements of an [enhanced][secure] electronic signature if expressly so agreed by the parties.

(3) The provisions of paragraph (2) do not apply to the following: [...].

References

A/CN.9/446, paras. 37-45 (draft article 1); and
A/CN.9/WG.IV/WP.73, para. 27.

Remarks

27. As opposed to unqualified "electronic signatures" dealt with in draft article 2, [enhanced] [secure] electronic signatures under draft article 6 present the advantage that, either through compliance with applicable regulations, or directly by contract, commercial parties can achieve certainty as to the legal effect of any given signing technique in advance of using that technique. The Working Group may wish to discuss whether limitations to party autonomy in that respect should be dealt with by the Uniform Rules or simply left to domestic law under paragraph (3) (see above, para. 14).

Article 7. Liability for [enhanced][secure] electronic signature

Variant A

Where the use of a[n] [enhanced][secure] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the purported signer is liable [to pay damages to compensate the relying party] for harm caused, unless the relying party knew or should have known that the signature was not that of the purported signer.

Variant B

Where the use of a[n] [enhanced][secure] electronic signature was unauthorized and the purported signer did not exercise reasonable care to avoid the unauthorized use of its signature and to prevent the addressee from relying on such a signature, the signature shall nevertheless be regarded as that of the purported signer, unless the relying party knew or should have known that the signature was not that of the purported signer.

References

A/CN.9/446, paras. 49-61 (draft article 3);
A/CN.9/WG.IV/WP.73, paras. 33-36;
A/CN.9/437, paras. 118-124 (draft article E); and
A/CN.9/WG.IV/WP.71, paras. 64-65.

Remarks

28. At its thirty-second session, the Working Group discussed whether the Uniform Rules should deal only with the attribution of secure electronic signatures (or digital signatures) or whether it should also address the issue of liability of the purported signer to the relying parties. It was emphasized that, in establishing the link between the electronic signature and the purported signer, the Uniform Rules should also create an incentive for the use of digital signatures by properly allocating liability for the loss caused to the relying party through the failure of the purported signer to exercise reasonable care and avoid the unauthorized use of its signature (see A/CN.9/446, para. 51).

29. The Working Group may wish to discuss the link between the Uniform Rules and article 13 of the Model Law. While article 13 of the Model Law deals with the attribution of the data message, the issue of attribution of an electronic signature is addressed in the definition of "[enhanced][secure] electronic signature" and in draft article 4.

30. Variant A limits the purported signer's liability to damages proved by the relying party, which may be computed on a tortious or contractual basis, depending on the circumstances. Variant B makes the purported signer liable for the contents of the data message.

Section III. Digital signatures supported by certificates

Article 8. Contents of [enhanced][secure] certificate

For the purposes of these Rules, a[n] [enhanced][secure] certificate shall, as a minimum:

(a) identify the certification authority issuing it;

(b) name or identify the [signer][subject of the certificate] or a device or electronic agent under the control of [the signer][the subject of the certificate][that person];

(c) contain a public key which corresponds to a private key under the control of the [signer][subject of the certificate];

(d) specify the operational period of the certificate;

(e) be digitally signed or otherwise secured by the certification authority issuing it;

[(f) specify the restrictions, if any, on the scope of use of the public key;] [and]

[(g) identify the algorithm to be applied].

References

A/CN.9/446, paras. 113-131 (draft article 8);
A/CN.9/WG.IV/WP.73, paras. 50-57;
A/CN.9/437, paras. 98-113 (draft article C); and
A/CN.9/WG.IV/WP.71, paras. 18-45 and 59-60.

Remarks

31. At its thirty-second session, the Working Group did not decide whether, as a matter of drafting, the Uniform Rules should refer to "the subject of the certificate"or specifically indicate that the subject should be a "person". With a view to improving the readability of the Uniform Rules, the term "signer" has been used consistently, while the term "subject" has also been kept for comparison. While the Uniform Rules could accommodate a reference to the notion of "person", extensive redrafting would be required to avoid ambiguity as to which person is intended to be covered. The definition of "signer" under draft article 1(h) indicates that the signer should be a "person".

Article 9. Effect of digital signatures supported by certificates

(1) In respect of all or any part of a data message, where the originator is identified by a digital signature, the digital signature [is a[n] [enhanced][secure] electronic signature][satisfies the conditions in article 7 of the UNCITRAL Model Law on Electronic Commerce] if:

(a) the digital signature was securely created during the operational period of a valid certificate and is securely verified by reference to the public key listed in the certificate; and

(b) the certificate binds a public key to [the signer's][a person's] identity by virtue of the fact that:

(i) the certificate was issued by a certification authority licensed by ... *[the enacting State specifies the organ or authority competent to license certification authorities and to promulgate regulations for the operation of licensed certification authorities]*; or

(ii) the certificate was issued by a certification authority accredited by a responsible accreditation body applying commercially appropriate and internationally recognized standards covering the trustworthiness of the certification authority's technology, practices and other relevant characteristics. A non-exclusive list of bodies or standards that comply with this paragraph may be published by ... *[the enacting State specifies the organ or authority competent to issue recognized standards for the operation of licensed certification authorities]*; or

(iii) the certificate was otherwise issued in accordance with commercially appropriate and internationally recognized standards[.][; or]

[(iv) sufficient evidence indicates that the certificate [accurately] binds the public key to the [signer's][subject's] identity.]

[(2) Where a data message is signed with a digital signature [created during the validity period of a certificate] that does not meet the requirements set forth in paragraph (1), the digital signature is regarded as a[n] [enhanced][secure] electronic signature if sufficient evidence indicates that [the certificate] accurately binds the public key to the identity of the [signer][subject of the certificate].]

(3) The provisions of this article do not apply to the following: [...].

References

A/CN.9/446, paras. 71-84 (draft article 5);
A/CN.9/WG.IV/WP.73, paras. 39-44; and
A/CN.9/437, paras. 43, 48 and 92.

Remarks

32. The opening words of paragraph (1) reflect the decision made by the Working Group at its thirty-second session (see A/CN.9/446, para. 76).

33. Digital signatures, if properly implemented, should constitute secure electronic signatures. However, a question is to determine when the implementation of a digital signature has been done in a manner such that it is entitled to secure status. Not all digital signatures verifiable with reference to a certificate are secure, especially where there is uncertainty as to whether

the identification or authentication of the signer or the public key is accurate. The primary factors that determine whether a digital signature is secure include: (1) whether the certification authority has properly identified the signer; (2) whether the certification authority has properly authenticated the signer's public key; (3) whether the signer's private key has been compromised; and (4) whether the process is trustworthy (e.g., whether the public key algorithm and the key length used are appropriate).

34. Paragraph (1) sets forth two basic criteria for determining when a digital signature qualifies as a secure electronic signature. The first criterion requires that the signature be created during the operational period of a valid certificate and be verified by reference to the public key listed in the certificate. The operational period of a certificate normally begins at the time it is issued and ends upon the earlier of expiration, revocation or suspension.

35. The second step involves providing assurance that the certificate itself accurately identifies a person as the signer in relation to a private key corresponding to the public key specified in the certificate. The trustworthiness of the certificate may be assessed by reference to standards, procedures, and other requirements specified by authorities recognized in the enacting State. Such standards may be established through accreditation of certification authorities by third parties, the voluntary licensing of certification authorities, or otherwise require compliance with rules adopted by the enacting State.

36. Alternatively, under paragraph (2), if a court or other trier of fact determines, as a matter of evidence, that the information stated in the certificate is in fact true, then the trustworthiness of the certificate is obvious. At this stage, however, the trier of fact is required to determine on a case-by-case basis whether the certificate was issued by a certification authority that properly identified the signer and authenticated the signer's public key.

37. Consistent with the "dual approach" taken by the Working Group, draft article 9 is intended to provide as much latitude as possible for making a determination as to the trustworthiness of a certificate issued by a certificate authority. This flexibility is particularly important in light of the fact that the use of digital signatures is new and the models for its use as well as its regulation have not yet fully developed. Thus, it is important to facilitate the increased use of digital signatures in electronic commerce, while at the same time establishing the standards necessary to make a presumptive determination as to the reliability of a digitally-signed message.

38. It is also important to note that while one of the options set forth in draft article 9 includes a judicial determination of the accuracy of a certificate, the other option presumes the accuracy of a certificate if it was issued by a certification authority accredited by the enacting State or if it otherwise meets certain standards established by the enacting State. In such a case, a judicial finding of accuracy is not required in order to qualify for a secure electronic signature status. The second option may be helpful to persons engaging in electronic commerce, who would know in advance of acting in reliance on a communication whether such action can be enforced. However, the presumption of accuracy may be rebutted by showing that a certificate issued by such an accredited certification authority is, in fact, not accurate or reliable (see A/CN.9/WG.IV/WP.73, paras. 39-44).

CHAPTER III. CERTIFICATION AUTHORITIES AND RELATED ISSUES

Article 10. Undertaking upon issuance of certificate

(1) By issuing a certificate, the certification authority undertakes [to any person who reasonably relies on the certificate] that:

(a) the certification authority has complied with all applicable requirements of [these Rules];

(b) all information in the certificate is accurate as of the date it was issued, [unless the certification authority has stated in the certificate that the accuracy of specified information is not confirmed];

(c) to the certification authority's knowledge, there are no known, material facts omitted from the certificate which would adversely affect the reliability of the information in the certificate; and

[(d) that if the certification authority has published a certification practice statement, the certificate has been issued by the certification authority in accordance with that certification practice statement.]

(2) By issuing a[n] [enhanced][secure] certificate, the certification authority makes the following additional undertakings in respect of the [signer][subject] identified in the certificate [to any person who reasonably relies on the certificate]:

(a) that the public key and private key of the [signer][subject] identified in the certificate constitute a functioning key pair; and

(b) that at the time of issuing the certificate, the private key is:

(i) that of the [signer][subject] identified in the certificate; and

(ii) corresponds to the public key listed in the certificate.

References

A/CN.9/446, paras. 134-145 (draft article 10);
A/CN.9/WG.IV/WP.73, paras. 61-63;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

39. Draft article 10 relies on a distinction between [enhanced][secure] certificates and a broader category of certificates. Depending on the decision to be made by the Working Group regarding the extent to which the Uniform Rules should deal with digital signatures as used for purposes other than establishing pre-determined equivalency with hand-written signatures, that distinction may not be needed (see above, para. 20).

Article 11. Contractual liability

Variant A

(1) As between a certification authority issuing a certificate and the holder of that certificate [or any other relying party having a contractual relationship with the certification authority], the rights and obligations of the parties [and any limitation thereon] are determined by their agreement [subject to applicable law].

[(2) Subject to article 10, a certification authority may, by agreement, exempt itself from liability for any loss [resulting from reliance on the certificate][due to defects in the information listed in the certificate, technical breakdowns or similar circumstances. However, the clause which limits or excludes the liability of the certification authority may not be invoked if exclusion or limitation of contractual liability would be grossly unfair, having regard to the purpose of the contract].]

[(3) The certification authority is not entitled to limit its liability if it is proved that the loss resulted from the act or omission of the certification authority done with intent to cause damage or recklessly and with knowledge that damage would probably result.]

Variant B

In accordance with applicable law, the rights and obligations of a certification authority, of a [signer][subject] identified in a certificate, and of any other party shall be governed by the agreement or agreements entered into by those parties to the extent that the agreement or agreements deal with those rights and obligations and any limitations thereon.

Variant C

Where agreements are entered into by a certification authority, a [signer][subject] identified in a certificate, or any other party, the rights and obligations of those parties and any limitation thereon which are dealt with in the agreements shall be governed by the agreements in accordance with and to the extent permitted by applicable law.

References

A/CN.9/446, paras. 146-154 (draft article 11);
A/CN.9/WG.IV/WP.73, paras. 64-65;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

40. Prior to considering the variants proposed for draft article 11, the Working Group may wish to discuss the question of whether draft article 11 should be retained as part of the Uniform Rules. At the thirty-second session of the Working Group, it was stated that the draft article dealt with matters that were better left to the contract and to the applicable law. In particular, it was observed that there might be no need to restate the principle of party autonomy, which was covered by article 4 of the Model Law; and that other matters dealt with in the draft article were interfering with national law on matters which might not lend themselves to unification. While leaving the issues of contractual liability to the contract and to the law applicable outside the Uniform Rules was found to be an acceptable alternative, the prevailing view was that it was worth trying to achieve a degree of unification on this important matter (see A/CN.9/446, para. 148).

Article 12. Liability of the certification authority to parties relying on certificate

(1) Subject to paragraph (2), where a certification authority issues a certificate, it is liable to any person who reasonably relies on that certificate for:

(a) errors in the certificate, unless the certification authority proves that it or its agents have taken [all reasonable][commercially reasonable] measures [that were appropriate for the purpose for which the certificate was issued, in the light of all circumstances] to avoid errors in the certificate;

(b) failure to register revocation of the certificate, unless the certification authority proves that it or its agents have taken [all reasonable][commercially reasonable] measures [that were appropriate for the purpose for which the certificate was issued, in the light of all circumstances] to register the revocation promptly upon receipt of notice of the revocation[; and

(c) the consequences of not following:

(i) any procedure set forth in the certification practice statement published by the certification authority; or

(ii) any procedure set forth in applicable law].

(2) Reliance on a certificate is not reasonable to the extent that it is contrary to the information contained [or incorporated by reference] in the certificate [or in a revocation list] [or in the revocation information]. [Reliance is not reasonable, in particular, if:

(a) it is contrary to the purpose for which the certificate was issued;

(b) it exceeds the value for which the certificate is valid; or

(c) [...].]"

References

A/CN.9/446, paras. 155-173 (draft article 12);
A/CN.9/WG.IV/WP.73, paras. 66-67;
A/CN.9/437, paras. 51-73 (draft article H); and
A/CN.9/WG.IV/WP.71, paras. 70-72.

Remarks

41. Draft article 12 reflects the decision made by the Working Group at its thirty-second session (A/CN.9/446, para. 173). At that session, the view was expressed that draft article 12 should apply only to certification authorities issuing identity certificates.

General remark regarding draft articles 13 to 16

42. At its previous session, for lack of sufficient time, the Working Group postponed its consideration of draft articles 13 to 16 to a future session (see A/CN.9/446, para. 174). Subject to editing, aimed mostly at ensuring the consistency of the various provisions included in the revised text of the Uniform Rules, the text of draft articles 13 to 16 in this note, is substantially identical to the text of those articles as set forth in document A/CN.9/WG.IV/WP.73.

Article 13. Revocation of certificate

(1) During the operational period of a certificate, the certification authority that issued the certificate must revoke the certificate in accordance with the policies and procedures governing revocation specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving:

(a) a request for revocation by the [signer][subject] identified in the certificate, and confirmation that the person requesting revocation is the [rightful] [signer][subject], or is an agent of the [signer][subject] with authority to request the revocation;

(b) reliable evidence of the [signer's][subject's] death if the [signer][subject] is a natural person; or

(c) reliable evidence that the [signer][subject] has been dissolved or has ceased to exist, if the [signer][subject] is a corporate entity.

(2) The [signer][subject] in relation to a certified key pair is under an obligation to revoke, or to request revocation of, the corresponding certificate where the [signer][subject] knows that the private key has been lost, compromised or is in danger of being misused in other respects. If the [signer][subject] fails to revoke, or to request revocation of, the certificate in such a situation, the [signer][subject] is liable to any person relying on a message as a result of the failure by the [signer][subject] to undertake such revocation.

(3) Regardless of whether the [signer][subject] identified in the certificate consents to the revocation, the certification authority that issued a certificate must revoke the certificate promptly upon acquiring knowledge that:

(a) a material fact represented in the certificate is false;

(b) the certification authority's private key or information system was compromised in a manner affecting the reliability of the certificate; or

(c) the [signer's][subject's] private key or information system was compromised.

(3) Upon effecting the revocation of a certificate under paragraph (3), the certification authority must notify the [signer][subject] and relying parties in accordance with the policies and procedures governing notice of revocation specified in the applicable certification practice statement, or in the absence of such policies and procedures, promptly notify the [signer] [subject] and promptly publish notice of the revocation if the certificate was published, and otherwise disclose the fact of revocation upon inquiry by a relying party.

(4) [As between the [signer][subject] and the certification authority,] the revocation is effective from the time when it is [received] [registered] by the certification authority.

[(5) As between the certification authority and any other relying party, the revocation is effective from the time it is [registered] [published] by the certification authority.]

References

A/CN.9/446, para. 174 (draft article 13);
A/CN.9/WG.IV/WP.73, para. 68;
A/CN.9/437, paras.125-139 (draft article F); and
A/CN.9/WG.IV/WP.71, paras. 66-67.

Remarks

43. Draft article 13 is intended to reflect the various views expressed at the thirty-first session of the Working Group by setting forth a default standard governing revocation of certificates. At all times, however, a certification authority can avoid the default standard by establishing procedures governing revocation in its certification practice statement, and following those procedures. As regards the time of effectiveness of a revocation, the Working Group may wish to decide whether a distinction should be drawn between the situation of the signer and that of any other relying party (see A/CN.9/437, para. 130).

Article 14. Suspension of certificate

During the operational period of a certificate, the certification authority that issued the certificate must suspend the certificate in accordance with the policies and procedures governing suspension specified in the applicable certification practice statement or, in the absence of such policies and procedures, promptly upon receiving a request to that effect by a person whom the certification authority reasonably believes to be the [signer][subject] identified in the certificate or a person authorized to act on behalf of that [signer][subject].

References

A/CN.9/446, para. 174 (draft article 14);
A/CN.9/WG.IV/WP.73, para. 69; and
A/CN.9/437, paras. 133-135 (draft article F).

Remarks

44. At its thirty-first session, the Working Group decided that the Uniform Rules should contain a provision on suspension of certificates (see A/CN.9/437, paras. 133-134). As regards the time of effectiveness of a suspension, the Working Group may wish to decide whether provisions should be added along the lines of the principles in paragraphs (4) and (5) of draft article 13.

Article 15. Register of certificates

(1) Certification authorities shall keep a publicly accessible electronic register of certificates issued, indicating the time when any individual certificate expires or when it was suspended or revoked.

(2) The register shall be maintained by the certification authority

Variant A for at least [30] [10] [5] years

Variant B for ... *[the enacting State specifies the period during which the relevant information should be maintained in the register]*

after the date of revocation or expiry of the operational period of any certificate issued by that certification authority.

Variant C in accordance with the policies and procedures specified by the certification authority in the applicable certification practice statement.

References

A/CN.9/446, para. 174 (draft article 15);
A/CN.9/WG.IV/WP.73, paras. 70-71;
A/CN.9/437, paras. 140-148 (draft article G); and
A/CN.9/WG.IV/WP.71, para. 68-69.

Remarks

45. At the thirty-first session of the Working Group, no objection of principle was raised to including in the Uniform Rules a provision on registration of certificates (see A/CN.9/437, para. 142). The proper maintenance of a widely accessible register (sometimes referred to as a "repository") featuring, in particular, a certificate revocation list (CRL) may be regarded as an important element in establishing the trustworthiness of digital signatures. When dealing with the ways in which such registers and CRLs should be maintained by certification authorities, the Working Group may wish to consider whether relying parties should be under an obligation to verify the status of the certificate by consulting the relevant register or CRL before they could rely on the validity of the certificate.

46. More generally, the Working Group may wish to discuss whether the Uniform Rules, in establishing minimum standards for the operation of certification authorities, should also deal with the rights and obligations of parties relying on certificates.

Article 16. Relations between parties relying on certificates and certification authorities

[(1) A certification authority is only allowed to request such information as is necessary to identify the [signer][subject of the certificate].

(2) Upon request, the certification authority shall deliver information about the following:

(a) the conditions under which the certificate may be used;

(b) the conditions associated with the use of digital signatures;

(c) the costs of using the services of the certification authority;

(d) the policy or practices of the certification authority with respect to the use, storage and communication of personal information;

(e) the technical requirements of the certification authority with respect to the communication equipment to be used by parties relying on certificates;

(f) the conditions under which warnings are given to parties relying on certificates by the certification authority in case of irregularities or faults in the functioning of the communication equipment;

(g) any limitation of the liability of the certification authority;

(h) any restrictions imposed by the certification authority on the use of the certificate; and

(i) the conditions under which the [signer][subject] is entitled to place restrictions on the use of the certificate.

(3) The information listed in paragraph (1) shall be delivered to the [potential] [signer] [subject] before a final agreement of certification is concluded. That information may be delivered by the certification authority by way of a certification practice statement.

(4) Subject to a [one-month] notice, the [signer][subject] may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received by the certification authority.

(5) Subject to a [three-month] notice, the certification authority may terminate the agreement for connection to the certification authority. Such notice of termination takes effect when received.]

References

A/CN.9/446, para. 174 (draft article 16);
A/CN.9/WG.IV/WP.73, para. 72;
A/CN.9/437, paras. 149-150 (draft article J); and
A/CN.9/WG.IV/WP.71, para. 76.

Remarks

47. At its thirty-first session, the Working Group noted that the various elements listed in draft article 15 should be placed in square brackets, to be considered by the Working Group at a later stage (see A/CN.9/437, para. 150).

CHAPTER IV. FOREIGN ELECTRONIC SIGNATURES

Article 17. Provision of services by foreign certification authorities

(1) Variant A Foreign [persons][entities] may become locally established as certification authorities or may provide certification services from another country without a local establishment if they meet the same objective standards [and follow the same procedures] as domestic entities and persons that may become certification authorities.

Variant B Subject to the laws of the enacting State, a foreign [person][entity] may:

(a) become locally established as a certification authority; or

(b) provide certification services without being established locally if it meets the same objective standards and follows the same procedures as domestic entities and persons that may become certification authorities.

Variant C Foreign [persons][entities] may not be denied the right to become locally established or to provide certification services solely on the grounds that they are foreign if they meet the same objective standards [and follow the same procedures] as domestic entities and persons that may become certification authorities.

[(2) Variant X The rule stated in paragraph (1) does not apply to the following: [...].

Variant Y Exceptions to the rule stated in paragraph (1) may be made to the extent required by national security.]

References

A/CN.9/446, paras. 175-188 (draft article 17);
A/CN.9/WG.IV/WP.73, para. 73;
A/CN.9/437, paras. 74-89 (draft article I); and
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

48. By allowing foreign entities to become established as certification authorities, draft article 17 merely states the principle that foreign entities should not be discriminated against, provided that they meet the standards set forth for domestic certification authorities. While that principle may be generally accepted, it may be of particular relevance to express it with respect to certification authorities, since certification authorities might be expected to operate

without necessarily having a physical establishment or other place of business in the country in which they operate.

Article 18. Endorsement of foreign certificates by domestic certification authorities

Variant A

Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as certificates subject to these Rules if they are recognized by a certification authority operating under ... *[the law of the enacting State]*, and that certification authority guarantees, to the same extent as its own certificates, the correctness of the details of the certificate as well as the certificate being valid and in force.

Variant B

Certificates issued by foreign certification authorities may be used for digital signatures on the same terms as certificates subject to these Rules on the basis of an appropriate guarantee provided by a certification authority operating under ... *[the law of the enacting State]*.

References

A/CN.9/446, paras. 189-195 (draft article 18);
A/CN.9/WG.IV/WP.73, para. 74;
A/CN.9/437, paras. 74-89 (draft article I); and
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

49. Draft article 18 enables a domestic certification authority to guarantee, to the same extent as its own certificates, the correctness of the details of the foreign certificate, and to guarantee that the foreign certificate is valid and in force. It refers to the matters referred to as "cross-certification" at the thirty-first session of the Working Group. Draft article 18 essentially contains a provision on the allocation of liability to the domestic certification authority in the event that the foreign certificate is found to be defective (see A/CN.9/437, paras. 77-78).

Article 19. Recognition of foreign certificates

Variant A

(1) Variant X

Certificates issued by foreign certification authorities shall not be precluded from having the same recognition as certificates issued by domestic certification authorities on the ground that they have been issued by foreign certification authorities.

Variant Y

Certificates issued by a foreign certification authority are recognized as legally equivalent to certificates issued by certification authorities

operating under ... *[the law of the enacting State]* if the practices of the foreign certification authority provide a level of reliability at least equivalent to that required of certification authorities under these Rules. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

(2) Signatures and records complying with the laws of another State relating to digital or other electronic signatures are recognized as legally equivalent to signatures and records complying with these Rules if the laws of the other State require a level of reliability at least equivalent to that required for such records and signatures under ... *[the Law of the enacting State]*. [Such recognition may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(2)[3] Digital signatures that are verified by reference to a certificate issued by a foreign certification authority shall [be][not be precluded from being] given effect [by courts and other finders of fact] if the certificate is as reliable as is appropriate for the purpose for which the certificate was issued, in light of all the circumstances.

(3)[4] Notwithstanding the preceding paragraph, Government agencies and parties to commercial and other transactions may specify that a particular certification authority, class of certification authorities or class of certificates must be used in connection with messages or signatures submitted to them.

Variant B

(1) Certificates issued by a foreign certification authority are recognized as legally equivalent to certificates issued by certification authorities operating under [*the law of the enacting State*] if the practices of the foreign certification authority provide a level of reliability at least equivalent to that required of certification authorities under these Rules.

[(2) The determination of equivalence described in paragraph (1) may be made by a published determination of the State or through bilateral or multilateral agreement with other States.]

(3) In the determination of equivalence, regard shall be had to the following factors :

(a) financial and human resources, including existence of assets within jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the liability of the certification authority and the law of enacting State.

Variant C

A foreign certification authority is considered reliable *[in the enacting State]* for the purpose of a certificate it issues to support signatures in relation data messages if, in issuing such a certificate, the certification authority complies with, and is subject at least to the same liabilities as those imposed by, these Rules and any domestic licensing regime applicable to a certificate of that type.

Variant D

(1) A foreign certification authority is considered reliable *[in the enacting State]* for the purpose of a certificate it issues to support signatures in relation data messages if, in issuing such a certificate, the certification authority provides a level of reliability [at least] equivalent to that [required] of domestic certification authorities issuing such certificates.

(2) In assessing a certification authority's level of reliability, regard shall be had to the following factors :

(a) financial and human resources, including existence of assets within jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the liability of the certification authority and the law of enacting State.

References

A/CN.9/446, paras. 196-207 (draft article 19);
A/CN.9/WG.IV/WP.73, para. 75;
A/CN.9/437, paras. 74-89 (draft article I); and
A/CN.9/WG.IV/WP.71, paras. 73-75.

Remarks

50. Draft article 19 refers to the matters referred to as "cross-border recognition" at the thirty-first session of the Working Group (see A/CN.9/437, paras. 77-78). Variant A is based on suggestion for a combination of paragraphs (1) and (2) made at the thirty-second session of the Working Group (see A/CN.9/446, paras. 197-204). Variant B provides an illustrative list of criteria to be taken into account in assessing the reliability of foreign certificates. Variants C and D focus on the recognition of the foreign certification authorities. It may be noted that, should the Working Group decide to include in the Uniform Rules criteria to be met by domestic certification authorities (see above, para. 19), there might be no need to provide for such criteria in draft article 19.

* * *

Notes

[1] Official Records of the General Assembly, Fifty-first Session, Supplement No. 17 (A/51/17), paras. 223-224.

[2] Ibid., Fifty-second Session, Supplement No. 17 (A/52/17), paras. 249-251.

UNITED
NATIONS

A

General Assembly

Distr.
LIMITED

A/CN.9/WG.IV/WP.77
25 May 1998

ORIGINAL: ENGLISH

UNITED NATIONS COMMISSION
ON INTERNATIONAL TRADE LAW
Working Group on Electronic Commerce
Thirty-third session
New York, 29 June - 10 July 1998

PROPOSAL BY THE UNITED STATES OF AMERICA

Note by the Secretariat

1. At the close of the thirty-second session of the Working Group, the proposal was made that the Working Group might wish to give preliminary consideration to undertaking the preparation of an international convention based on provisions of the Model Law and of the Uniform Rules. It was agreed that the topic might need to be taken up as an agenda item at the next session of the Working Group on the basis of more detailed proposals possibly to be made by interested delegations. However, the preliminary conclusion of the Working Group was that the preparation of a convention should in any event be regarded as a project separate from both the preparation of the Uniform Rules and any other possible addition to the Model Law. Pending a final decision as to the form of the Uniform Rules, the suggestion to prepare a convention at a later stage should not distract the Working Group from its current task, which was to focus on the preparation of draft uniform rules on digital and other electronic signatures, and from its current working assumption that the Uniform Rules would be in the form of draft legislative provisions. It was generally understood that the possible preparation of a draft convention should not be used as a means of reopening the issues settled in the Model Law, which might negatively affect the increased use of that already successful instrument (A/CN.9/446, para. 212).

2. Following the thirty-second session of the Working Group, the Secretariat received from the delegation of the United States of America a proposal for a draft international convention on electronic transactions, together with the text of a "United States Government Non-paper on Electronic Transactions" that explains the rationale and purpose of the proposed convention. The text of that proposal and the corresponding "non-paper" are reproduced in the annex to this note as they were received by the Secretariat.

V.98-53830

ANNEX

DRAFT INTERNATIONAL CONVENTION ON ELECTRONIC TRANSACTIONS

CHAPTER I

Proposed Goal of Chapter I: To set forth any necessary definitions. To be developed after Chapter II and III.

CHAPTER II

Proposed Goal of Chapter II: In order to implement the legal rules articulated in the second section, as set forth below, it may be necessary for states to review their existing and proposed legislation to assure that it is appropriately tailored to electronic transactions. In order to facilitate such review and adoption on a harmonized basis, the following general obligations are proposed as the framework states should use to support electronic transactions on a global basis.

POSSIBLE LANGUAGE:

II. General Obligations

To encourage the free flow of electronic transactions and to avoid the creation of barriers to these transactions, subject to overriding public policy, the Contracting States hereby agree as follows:

> **Modification of Existing Rules and Minimal Adoption of New Rules** - States shall make only those changes to their laws that are necessary to support the use of electronic transactions. Existing rules should be modified and new rules adopted only in co-operation with the private sector and where necessary.

Contracting States recognize that parties to a transaction may determine the method of authentication for that transaction. Recognizing that parties may make this determination and recognizing that this determination should have the legal effect intended by the parties, the Contracting States agree as follows:

> **Party Autonomy** - Parties to a transaction should be permitted, to the maximum extent possible, to determine by contract the appropriate technological and business methods of authentication with the assurance that those means will be recognized as legally binding, whether or not those technological and business means are specifically addressed by legislation or regulation. The terms of any agreement (including closed systems) between parties governing their transaction should be enforced without regard to any statutory framework governing electronic authentication.

Further, Contracting States recognize that cryptography is not the sole means of proving the source or existence of a message. Recognizing that parties may establish the source or existence of a message in different ways, Contracting States agree as follows:

All Authentication Technologies and Business Methods May Be Evidence of Authenticity - Where the law requires evidence of the authenticity or integrity of a message, a party shall be permitted to use any authentication technology or business method, whether or not such authentication technology or business method has been specifically addressed by legislation or regulation.

Electronic Authentication methods should not be "locked in" through legislative fiat but rather should allow for changing applications for existing and future technologies. Therefore, the Contracting States agree that:

Technology Neutrality - Any rules should neither require nor hinder the use or development of authentication technologies. States should anticipate that authentication methods will change over time and avoid legislation that might preclude innovation or new applications. States should avoid laws that intentionally or unintentionally drive the private sector to adopt only one particular technology for electronic authentication to the exclusion of other viable authentication methods.

Authentication technologies may be implemented and used by businesses in ways that were not originally envisaged when legislation was passed. Recognizing that technology may be used for purposes such as establishing age or authority, which may go beyond verifying identity and achieving non-repudiation, and recognizing that business models for authentication may not use third parties, the Contracting States agree that:

Implementation Neutrality - Any rules should neither require nor hinder the use or development of new or innovative business applications or implementation models.

To remove barriers to the free flow of electronic transactions and to avoid the creation of new barriers, subject to overriding public policy, the Contracting States agree that:

Non-Discrimination - States shall accord to providers and users of authentication technologies and business methods of another state treatment no less favourable than it accords in like circumstances to its own providers and users of authentication technologies and business methods.

Avoid Unnecessary Barriers to Trade - States should enhance the flow of cross-border electronic transactions and not create unnecessary barriers to trade.

CHAPTER III

Proposed Goal of Chapter III: To recognize the acceptability of electronic signatures for legal and commercial purposes, define the characteristics of a valid electronic writing and an original document, support the admission of electronic evidence and the electronic retention of records. These provisions would be drawn from the enabling provisions of the UNCITRAL Model Law on Electronic Commerce.

POSSIBLE LANGUAGE:

III. Specific Obligations

Contracting States recognize the work of the United Nations Commission on International Trade Law and the importance of establishing its governing provisions on a uniform, international basis. Contracting States also recognize information is increasingly generated, stored, sent, received or otherwise processed electronically, rather than in a paper based form. Recognizing these important business practices, the Contracting States hereby agree on the following:

Legal Recognition of Data Messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message. [Source Model Law on Electronic Commerce, article 5].

Formation and Validity of Contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following ... [limited exception]. [Source: Model Law on Electronic Commerce, article 11].

Contracting States recognize that the formal requirements that currently exist under many legal regimes may constitute insurmountable barriers to the conduct of electronic transactions on an international basis. As a result, there is a paramount need for assuring that electronically transmitted messages are allowed to satisfy these formal requirements subject to overriding public policy. Therefore, the Contracting States agree as follows:

Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following ... [limited exception]. [Source: Model Law on Electronic Commerce, article 6].

Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is a reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following ... [limited exception]. [Source: Model Law on Electronic Commerce, article 7].

Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following ... [limited exception]. [Source: Model Law on Electronic Commerce, article 8].

The Contracting States recognize that the inability of parties to prove the existence of electronic transactions in the event of dispute and formal judicial proceedings may itself be an inhibition to the conduct of electronic transactions. To assure the legal equivalence of electronic documents with paper based ones, the Contracting States agree that:

Admissibility and Evidential Weight of Data Messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor. [Source: Model Law on Electronic Commerce, article 9]

Contracting States further recognize that requirements for record retention, which exist both as a matter of law and business practice, may prove to be obstacles for electronic transactions. The Contracting States agree, therefore, that:

Retention of Data Messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy these requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions in subparagraphs (a), (b) and (c) of paragraph 1 are met. [Source: Model Law on Electronic Commerce Article 10]

United States Government
Non-Paper on Electronic Transactions

To encourage electronic transactions, the United States supports both a domestic and global uniform legal framework that recognizes, facilitates, and enforces electronic transactions worldwide.

I.

The United Nations Commission on International Trade Law (UNCITRAL) has completed work on a Model Law on Electronic Commerce that supports the commercial use of international contracts in electronic commerce. The Model Law establishes rules and norms that define the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes, and supports the admission of computer evidence. It also validates and recognizes contracts formed through electronic means, setting default rules for contract formation and the governance of electronic contract performance.

While many countries, including the United States, are using the Model Law as a basis for updating their commercial laws, many countries are not. The United States Government supports the adoption of the enabling principles that are contained in the Model Law through a binding international agreement as a start to defining an international set of uniform commercial principles for electronic commerce.

II.

On the international level, a number of countries are considering or have enacted digital signature legislation to specifically address authentication methods including digital signatures. Recently, UNCITRAL began work in the authentication area, specifically including digital signatures, and is currently considering model statutory provisions.

Since UNCITRAL began its work last year, new models for the implementation and use of digital signature technology have emerged. The expanding array of authentication methods and the complexity of their commercial use raise concerns about fashioning detailed legal rules at this point in such areas as, for example, certificate authorities and liability. In the United States, most states to consider digital signature legislation recently have rejected statutory enactments setting forth specific rules for digital signatures, opting instead for more generalized enabling and supporting legislation that supports the use of digital signatures and other authentication technologies, but which otherwise does not impose liability or licensing schemes.

This new legislative approach reflects important evolutionary market changes. In particular, the market appears unlikely to settle on one universal authentication mechanism or model of implementation in the near future. Parties appear headed toward a choice between different types

of authentication regimes, depending on the nature of the transaction and upon the prior relationship, if any, among the parties to the transaction. For example, a large company may choose one authentication method for the electronic system used to procure goods from supplie but a different method for on-line purchases by its customers.

Like other aspects of electronic commerce, authentication methods and technologies are developing rapidly. In the area of digital signatures, the technology is being implemented in ways that are different from the public key infrastructures envisaged when the first digital signature legislation was passed. For example, digital signatures may be used for purposes suc as establishing age or authority, which may go beyond verifying identity and achieving nonrepudiation. In addition, much of its use is in closed rather than in open systems. There is also recognition that digital signatures are being used for a great number of business purposes apart from those originally envisaged; for example, minimal value certificates are already being issued on a wide scale basis.

The U.S. Government supports the development of structures that will support a variety of authentication methods and technologies as well as a variety of implementation models. Fashioning rules that would govern digital signature technology or any other single authentication technology, to the exclusion of other authentication approaches, would inhibit rather than encourage the growth of electronic commerce. Nevertheless, the U.S. Government recognizes the valuable dialogue supported by UNCITRAL on these issues.

The U.S. Government believes that UNCITRAL should consider giving priority attention to an International Convention on Electronic Transactions. The Convention would remove paper-based obstacles to electronic transactions, and address electronic authentication issues.

III.

UNCITRAL should work towards a binding Convention on electronic transactions that would have two elements:

Part A: General Obligations -- These would include: minimal modification to existing legal rules and minimal adoption of new rules; technology and implementation neutrality; a non-discriminatory approach toward authentication technologies and business applications from oth countries; the avoidance of unnecessary barriers to trade. In addition:

> Party Autonomy-- Parties to a transaction should be permitted, to the maximum extent possible, to determine by contract the appropriate technological and business methods of authentication with the assurance that those means will be recognized as legally binding, whether or not those technological and business means are specifically addressed by legislation or regulation. The terms of any agreement (including closed systems) between parties governing their transaction should be enforced without regard to any statutory framework governing electronic authentication.
>
> All Authentication Technologies and Business Methods May Be Evidence of Authenticity Where the law requires evidence of the authenticity or integrity of a message, a party shall be permitted to use any authentication technology or business method to try to prove authenticity, whether or not such authentication technology or business method has been

specifically addressed by legislation or regulation. (As with the authentication of physical documents, a party denying the agreement could introduce evidence disputing its authenticity or integrity and the issue would be resolved by the trier of fact.)

Part B: Adoption of Key Elements of the Model Law on Electronic Commerce -- Enabling provisions drawn from the provisions of the UNCITRAL Model Law on Electronic Commerce would define an international set of uniform commercial principles for electronic commerce. The Convention would recognize the acceptability of electronic signatures for legal and commercial purposes, define the characteristics of a valid electronic writing and an original document and support the admission of electronic evidence and the retention of electronic records.